Active directory - Excessive amount of domain admins

Description

Recommendation

How to test for

Domain admins can be counted in several different ways. For example between enabled and disabled users. Or by including users who are admins through inheretance of group memberships.

Within Active Directory, there are three built-in groups that comprise the highest privilege groups in the directory: the Enterprise Admins (EA) group, the Domain Admins (DA) group, and the built-in Administrators (BA) group.

There are many more groups that can be sensitive. You can read about those here: https://adsecurity.org/?p=3700. But we will only list users of these three groups. This is kind of a bare minimum test.

Therefore we will check who are members in these groups. If the query is run in Neo4j it can be exported using

```
 MATCH p=(n:User )-[r:MemberOf]->(m:Group {name : "ADMINISTRATORS@domain.local"}) RETURN n.displayname, n.name,n.description,n.lastlo
MATCH p=(n:User )-[r:MemberOf]->(m:Group {name : "DOMAIN ADMINS@domain.local"}) RETURN n.displayname, n.name,n.description,n.lastlog
MATCH p=(n:User )-[r:MemberOf]->(m:Group {name : "ENTERPRISE ADMINS@domain.local"}) RETURN n.displayname, n.name,n.description,n.las
```

The query can then be run executed like this, but of course with the correct domain name

```
cat query.txt |  /usr/share/neo4j/bin/cypher-shell --non-interactive -u neo4j -p PASSWORD --format plain > file.csv
```

This will check for all objects that are members of the Domain admins group. This will include other groups and computers.

```
MATCH (n:Group) WHERE n.objectsid =~ "(?i)S-1-5-.*-512" WITH n MATCH p=(n)<-[r:MemberOf]-(m) RETURN p
```